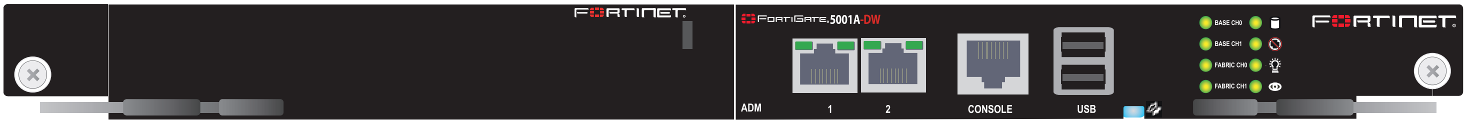
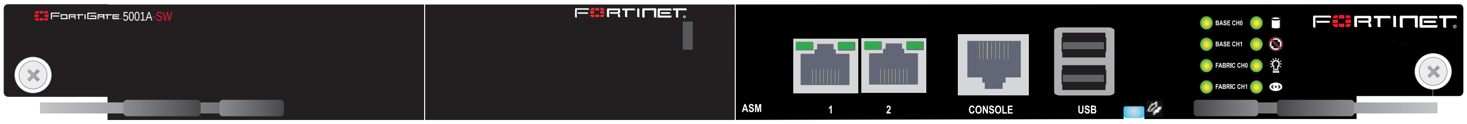
FortiGate-5001A

Security System Guide



FortiGate-5001A-DW



FortiGate-5001A-SW

A detailed guide to the FortiGate-5001A-DW and FortiGate-5001A-SW Security Systems. This *FortiGate-5001A Security System Guide* describes FortiGate-5001A hardware features, how to install a FortiGate-5001A board in a FortiGate-5000 series chassis, and how to configure the FortiGate-5001A security system for your network.

The most recent versions of this and all FortiGate-5000 series documents are available from the FortiGate-5000 page of the Fortinet Technical Documentation web site (http://docs.forticare.com).

Visit http://support.fortinet.com to register your FortiGate-5001A security system. By registering you can receive product updates, technical support, and FortiGuard services.

UNIFIED THREAT MANAGEMENT SOLUTIONS

FortiGate-5001A Security System Guide

01-30000-83456-20081023

Warnings and cautions

Only trained and qualified personnel should be allowed to install or maintain FortiGate-5000 series equipment. Read and comply with all warnings, cautions and notices in this document.

⚠ **CAUTION:** Risk of Explosion if Battery is replaced by an Incorrect Type. Dispose of Used Batteries According to the Instructions.

⚠ **Caution:** You should be aware of the following cautions and warnings before installing FortiGate-5000 series hardware

- Turning off all power switches may not turn off all power to the FortiGate-5000 series equipment. Some circuitry in the FortiGate-5000 series equipment may continue to operate even though all power switches are off.
- Many FortiGate-5000 components are hot swappable and can be installed or removed while the power is on. But some of the procedures in this document may require power to be turned off and completely disconnected. Follow all instructions in the procedures in this document that describe disconnecting FortiGate-5000 series equipment from power sources, telecommunications links and networks before installing, or removing FortiGate-5000 series components, or performing other maintenance tasks. Failure to follow the instructions in this document can result in personal injury or equipment damage.
- Install FortiGate-5000 series chassis at the lower positions of a rack to avoid making the rack top-heavy and unstable.
- Do not insert metal objects or tools into open chassis slots.
- Electrostatic discharge (ESD) can damage FortiGate-5000 series equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist strap and attaching it to an available ESD connector such as the ESD sockets provided on FortiGate-5000 series chassis.
- Make sure all FortiGate-5000 series components have reliable grounding. Fortinet recommends direct connections to the building ground.
- If you install a FortiGate-5000 series component in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Make sure the operating ambient temperature does not exceed Fortinet’s maximum rated ambient temperature.
- Installing FortiGate-5000 series equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- FortiGate-5000 series chassis should be installed by a qualified electrician.
- FortiGate-5000 series equipment shall be installed and connected to an electrical supply source in accordance with the applicable codes and regulations for the location in which it is installed. Particular attention shall be paid to use of correct wire type and size to comply with the applicable codes and regulations for the installation / location. Connection of the supply wiring to the terminal block on the equipment may be accomplished using Listed wire compression lugs, for example, Pressure Terminal Connector made by Ideal Industries Inc. or equivalent which is suitable for AWG 10. Particular attention shall be given to use of the appropriate compression tool specified by the compression lug manufacturer, if one is specified.

Contents

FortiGate-5001A security system

The FortiGate-5001A security system is a high-performance Advanced Telecommunications Computing Architecture (ACTA) compliant FortiGate security system that can be installed in any ACTA chassis including the FortiGate-5140, FortiGate-5050, or FortiGate-5020 chassis.

Two FortiGate-5001A models are available:

- The FortiGate-5001A-DW (double-width) board includes a double-width Advanced Mezzanine Card (AMC) opening. You can install a supported FortiGate ADM module such as the FortiGate-ADM-XB2 or the FortiGate-ADM-FB8 in the AMC opening. The FortiGate-ADM-XB2 adds two accelerated 10-gigabit interfaces to the FortiGate-5001A board and the FortiGate-ADM-FB8 adds 8 accelerated 1-gigabit interfaces.
- The FortiGate-5001A-SW (single-width) includes a single-width AMC opening. You can install a supported FortiGate ASM module such as the FortiGate-ASM-FB4 or the FortiGate-ASM-S08 in the AMC opening. The FortiGate-ASM-FB4 adds four accelerated 1-gigabit interfaces to the FortiGate-5001A board and the FortiGate-ADM-S08 adds a removable hard disk that you can use to store log files and content archives.

Other than the double-width and single-width AMC openings, the FortiGate-5001A-DW and SW models have the same functionality and performance.

The FortiGate-5001A security system contains two front panel 1-gigabit ethernet interfaces, two base backplane 1-gigabit interfaces, and two fabric backplane 1-gigabit interfaces. Use the front panel interfaces for connections to your networks and the backplane interfaces for communication across the ACTA chassis backplane.

If you install a FortiGate-RTM-XB2 module for each FortiGate-5001A board, the FortiGate-5001A fabric interfaces can operate at 10 Gbps. The FortiGate-RTM-XB2 also provides NP2-accelerated network processing for eligible traffic passing through the FortiGate-RTM-XB2 interfaces.

You can also configure two or more FortiGate-5001A boards to create a high availability (HA) cluster using the base or fabric backplane interfaces for HA heartbeat communication through the chassis backplane, leaving front panel interfaces available for network connections.

Note: In most cases the base backplane interfaces are used for HA heartbeat communication and the fabric backplane interfaces are used for data communication.

The FortiGate-5001A board also supports high-end FortiGate features including 802.1Q VLANs, multiple virtual domains, 802.3ad aggregate interfaces, and FortiOS Carrier.

Figure 1: FortiGate-5001A-DW front panel

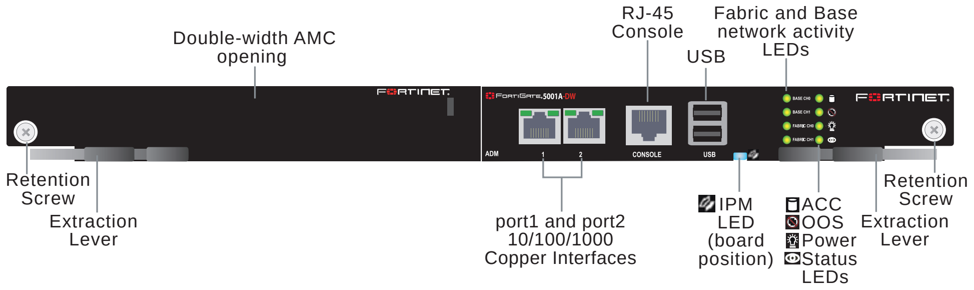
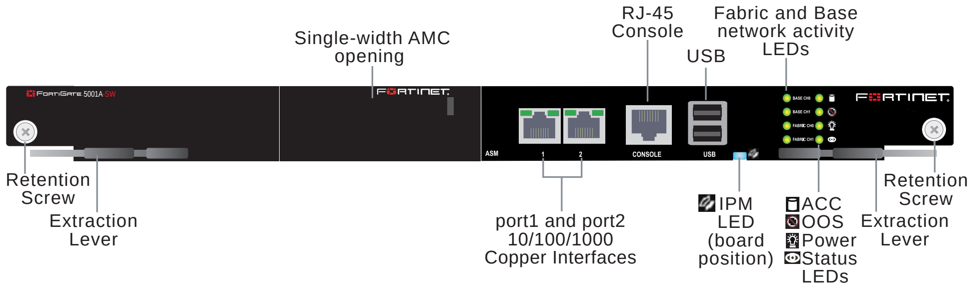


Figure 2: FortiGate-5001A-SW front panel



The FortiGate-5001A board includes the following features:

- Two front panel 10/100/1000Base-T copper 1-gigabit ethernet interfaces.
- Two base backplane 1-gigabit interfaces (base CH0 and Base CH1 on the front panel and base1 and base2 in the firmware) for HA heartbeat and data communications across the FortiGate-5000 chassis backplane.
- Two fabric backplane interfaces (Fabric CH0 and Fabric CH1 on the front panel and fabric1 and fabric2 in the firmware) for HA heartbeat and data communications across the FortiGate-5000 chassis backplane. The fabric backplane interfaces operate at 1 Gbps. If you install a FortiGate-RTM-XB2 module the fabric backplane interfaces operate at 10 Gbps.
- One double-width AMC opening (FortiGate-5001A-DW board).
- One single-width AMC opening (FortiGate-5001A-SW board).
- RJ-45 RS-232 serial console connection.
- 2 USB connectors.
- Mounting hardware.
- LED status indicators.

Front panel LEDs and connectors

From the FortiGate-5001A font panel you can view the status of the front panel LEDs to verify that the board is functioning normally. You also connect the FortiGate-5001A board to your network through the front panel 10/100/1000 ethernet connectors. The front panel also includes the RJ-45 console port for connecting to the FortiOS CLI and two USB ports. The USB ports can be used with any USB key for backing up and restoring configuration files. For information about using the using a USB key with a FortiGate unit, see the *FortiGate-5000 Series Firmware and FortiUSB Guide*.

LEDs

Table 1 lists and describes the FortiGate-5001A LEDs.

Table 1: FortiGate-5001A LEDs

LED	State	Description
1, 2 (Left LED)	Green	The correct cable is connected to the interface and the connected equipment has power.
	Flashing Green	Network activity at the interface.
	Off	No link is established.
1, 2 (Right LED)	Green	Connection at 1 Gbps.
	Amber	Connection at 100 Mbps.
	Off	Connection at 10 Mbps.
Base CH0	Green	Base backplane interface 0 (base1) is connected at 1 Gbps.
	Flashing Green	Network activity at base backplane interface 0.
Base CH1	Green	Base backplane interface 1 (base2) is connected at 1 Gbps.
	Flashing Green	Network activity at base backplane interface 1.
Fabric CH0	Off	Fabric backplane interface 0 (fabric1) is connected at 10 Gbps.
	Flashing Green	Network activity at fabric backplane interface 0.
Fabric CH1	Off	Fabric backplane interface 1 (fabric2) is connected at 10 Gbps.
	Flashing Green	Network activity at fabric backplane interface 1.
ACC	Off or Flashing green	The ACC LED flashes green when the FortiGate-5001A board accesses the FortiOS flash disk. The FortiOS flash disk stores the current FortiOS firmware build and configuration files. The system accesses the flash disk when starting up, during a firmware upgrade, or when an administrator is using the CLI or GUI to change the FortiOS configuration. Under normal operating conditions this LED flashes occasionally, but is mostly off.
OOS (Out of Service)	Off	Normal operation.
	Green	A fault condition exists and the FortiGate-5001A blade is out of service (OOS). This LED may also flash very briefly during normal startup.
Power	Green	The FortiGate-5001A board is powered on.
Status	Off	The FortiGate-5001A board is powered on.
	Flashing Green	The FortiGate-5001A is starting up. If this LED is flashing at any time other than system startup, a fault condition may exist.
IPM	Blue	The FortiGate-5001A is ready to be hot-swapped (removed from the chassis). If the IPM light is blue and no other LEDs are lit the FortiGate-5001A board has lost power.
	Flashing Blue	The FortiGate-5001A is changing from hot swap to running mode or from running mode to hot swap. This happens when the FortiGate-5001A board is starting up or shutting down.
	Off	Normal operation. The FortiGate-5001A board is in contact with the chassis backplane.

Connectors

Table 2 lists and describes the FortiGate-5001A connectors.

Table 2: FortiGate-5001A connectors

Connector	Type	Speed	Protocol	Description
1, 2	RJ-45	10/100/1000 Base-T	Ethernet	Copper 1-gigabit connection to 10/100/1000Base-T copper networks.
CONSOLE	RJ-45	9600 bps 8/N/1	RS-232 serial	Serial connection to the command line interface.
USB	USB			FortiUSB key firmware updates and configuration backup.

Base backplane communication

The FortiGate-5001A base backplane 1-gigabit interfaces can be used for HA heartbeat communication between FortiGate-5001A boards installed in the same or in different FortiGate-5000 chassis. You can also configure FortiGate-5001A boards to use the base backplane interfaces for data communication between FortiGate boards. To support base backplane communications your FortiGate-5140 or FortiGate-5050 chassis must include one or more FortiSwitch-5003 boards, FortiSwitch-5003A boards, or other 1-gigabit base backplane switching boards installed in the chassis in base slots 1 and 2. The FortiGate-5020 chassis supports base backplane communication with no additions or changes to the chassis.

For information about base backplane communication in FortiGate-5140 and FortiGate-5050 chassis, see the *FortiGate-5000 Backplane Communication Guide*. For information about the FortiSwitch-5003 board, see the *FortiSwitch-5003 System Guide*. For information about the FortiSwitch-5003A board, see the *FortiSwitch-5003A System Guide*.

Fabric backplane communication

The FortiGate-5001A fabric backplane interfaces can be used for data communication or HA heartbeat communication between FortiGate-5001A boards installed in the same or in different FortiGate-5000 chassis. To support 1-gigabit fabric backplane communications your FortiGate-5140 or FortiGate-5050 chassis must include one or more FortiSwitch-5003A boards or other 1-gigabit fabric backplane switching boards installed in the chassis in fabric slots 1 and 2. The FortiGate-5020 chassis does not support fabric backplane communications.

For information about fabric backplane communication in FortiGate-5140 and FortiGate-5050 chassis, see the *FortiGate-5000 Backplane Communication Guide*. For information about the FortiSwitch-5003A board, see the *FortiSwitch-5003A System Guide*.

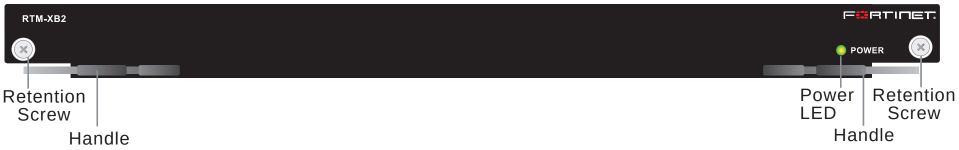
FortiGate-RTM-XB2

The FortiGate-RTM-XB2 module provides two 10-gigabit fabric backplane interfaces and NP2 processor acceleration for FortiGate-5001A fabric interfaces. For 10-gigabit fabric backplane communications, each FortiGate-5001A board requires one FortiGate-RTM-XB2 module. The FortiGate-RTM-XB2 module is an ATCA rear transition module (RTM) that installs into an RTM slot at the back of a FortiGate-5140 and FortiGate-5050 chassis.

To support 10-gigabit fabric backplane communications your FortiGate-5140 or FortiGate-5050 chassis must also include one or more FortiSwitch-5003A boards or other 10-gigabit fabric backplane switching boards installed in the chassis in fabric slots 1 and 2.

Note: On some versions of the FortiGate-5001A firmware, when a FortiGate-5001A board starts up with a FortiGate-RTM-XB2 module installed, the fabric1 and fabric2 interfaces are replaced with interfaces that are named RTM/1 and RTM/2 to indicate the presence of the FortiGate-RTM-XB2 module. Configuration settings that include the fabric1 and fabric2 interface names will have to be changed to use the RTM/1 and RTM/2 interface names.

Figure 3: FortiGate-RTM-XB2 front panel



The FortiGate-RTM-XB2 NP2 processors provide hardware accelerated network processing for eligible traffic passing through the FortiGate-RTM-XB2 interfaces. For information about Fortinet NP2 processor acceleration, see the *Fortinet Hardware Acceleration Technical Note*.

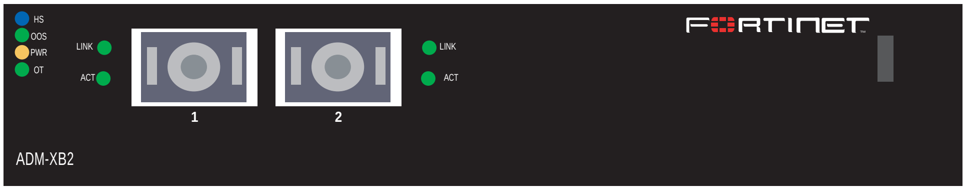
Follow the instructions in the *FortiGate-RTM-XB2 System Guide* to install the FortiGate-RTM-XB2 module.

AMC modules

You can install one FortiGate AMC Double width Module (ADM) in the FortiGate-5001A-DW front panel AMC double-width opening. For example:

- The FortiGate-ADM-XB2, provides 2 NP2 accelerated XFP 10-gigabit interfaces.
- The FortiGate-ADM-FB8, provides 8 NP2 accelerated SFP 1-gigabit interfaces.

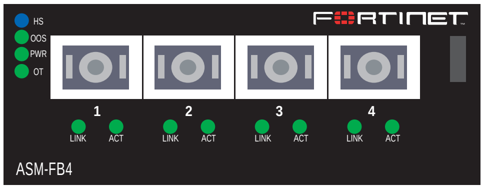
Figure 4: FortiGate-ADM-XB2



You can install one FortiGate AMC Single width Module (ASM) in the FortiGate-5001A-SW front panel AMC single-width opening. For example:

- The FortiGate-ASM-FB4, provides 4 NP2 accelerated SFP 1-gigabit interfaces.
- The FortiGate-ASM-S08, provides adds a removable hard disk that you can use to store log files and content archives.

Figure 5: FortiGate-ASM-FB4



Note: You can operate a FortiGate-5001A board with both a FortiGate-RTM-XB2 module and a supported FortiGate AMC module installed at the same time.

Hardware installation

Before use, the FortiGate-5001A board must be correctly inserted into an Advanced Telecommunications Computing Architecture (ACTA) chassis such as the FortiGate-5140, FortiGate-5050, or FortiGate-5020 chassis.

Before inserting the board into a chassis you should make sure the SW-11 switch is set correctly.

In the available Advanced Mezzanine Card (AMC) double-width module (ADM) opening on the FortiGate-5001A-DW front panel you can install a supported FortiGate ADM module such as the FortiGate-ADM-XB2 or the FortiGate-ADM-FB8.

In the available AMC single-width module (ASM) opening on the FortiGate-5001A-SW front panel you can install a supported ASM module such as the FortiGate-ASM-FB4 or the FortiGate-ASM-S08.

Caution: If you are installing a FortiGate-RTM-XB2 module you should install the FortiGate-RTM-XB2 module first, before you install the FortiGate-5001A board to avoid possible damage. Follow the instructions in the *FortiGate-RTM-XB2 System Guide* to install the FortiGate-RTM-XB2 module.

Caution: Because FortiGate-5001A boards do not support hot swapping AMC modules, the FortiGate-5001A board must be disconnected from power before you install a FortiGate AMC module. Also, the FortiGate-5001A-DW left (top) handle must be opened to install a FortiGate AMC module. See “Installing and removing AMC modules” on page 20.

Caution: Do not operate the FortiGate-5001A board with an open AMC opening. For optimum cooling performance and safety, the AMC opening must contain an AMC slot filler panel or a FortiGate AMC module.

Note: FortiGate-5001A boards are hot swappable even if the FortiGate-5001A board contains an AMC module and you have installed a FortiGate-RTM-XB2 module for the FortiGate-5001A board.

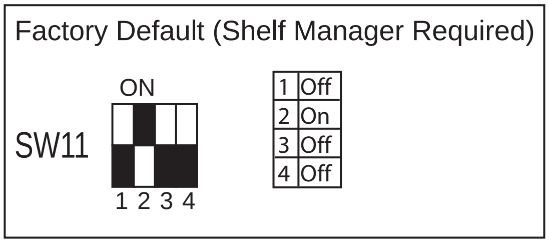
This section describes:

- Changing FortiGate-5001A SW11 switch settings
- FortiGate-5001A mounting components
- Inserting a FortiGate-5001A board
- Removing a FortiGate-5001A board
- Resetting a FortiGate-5001A board
- Installing and removing AMC modules
- Troubleshooting

Changing FortiGate-5001A SW11 switch settings

The SW11 switch on the FortiGate-5001A board is factory set by Fortinet to detect a shelf manager (Figure 6). This is the correct setting if you are installing the FortiGate-5001A board in a chassis that contains an operating shelf manager (such as the FortiGate-5140 or FortiGate-5050 chassis).

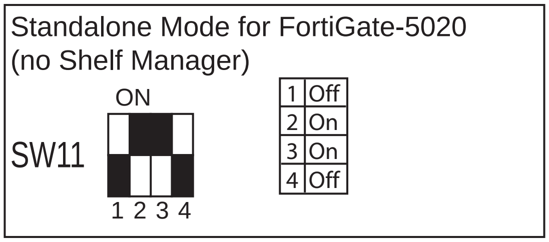
Figure 6: FortiGate-5140 and 5050 setting for SW11 (factory default shelf manager mode)



1	Off
2	On
3	Off
4	Off

By default a FortiGate-5001A board will not start up if the board is installed in a chassis, such as a FortiGate-5020, that does not contain a shelf manager or that contains a shelf manager that is not operating. Before installing a FortiGate-5001A in a FortiGate-5020 chassis or a chassis that does not contain an operating shelf manager you must change the SW11 switch setting as shown in Figure 7.

Figure 7: FortiGate-5020 setting for SW11 (standalone mode)



1	Off
2	On
3	On
4	Off

In all cases you should confirm that you have the correct SW11 setting before installing the board in a chassis.

Table 3: FortiGate-5001A SW11 settings for different chassis

Chassis	Correct SW11 Setting		Result of wrong jumper setting
FortiGate-5140 or 5050 or any ACTA chassis with an operating shelf manager (factory default shelf manager mode).	**1**	**Off**	Shelf manager cannot find FortiGate-5001A board. No shelf manager information about the FortiGate-5001A board available.
	2	**On**	
	3	**Off**	
	4	**Off**	
FortiGate-5020 or any ACTA chassis without an operating shelf manager (standalone mode).	**1**	**Off**	FortiGate-5001A board will not start up.
	2	**On**	
	3	**On**	
	4	**Off**	

Note: If the shelf manager in a FortiGate-5140 or FortiGate-5050 chassis is missing or not functioning, FortiGate-5001A boards with factory default SW11 settings will not start up.

To change or verify the SW11 switch setting

To complete this procedure, you need:

- A FortiGate-5001A board
- A tool for changing the SW11 switch setting (optional)
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

Caution: FortiGate-5001A boards must be protected from static discharge and physical shock. Only handle or work with FortiGate-5001A boards at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate-5001A boards.

1 Attach the ESD wrist strap to your wrist and to an available ESD socket or wrist strap terminal.

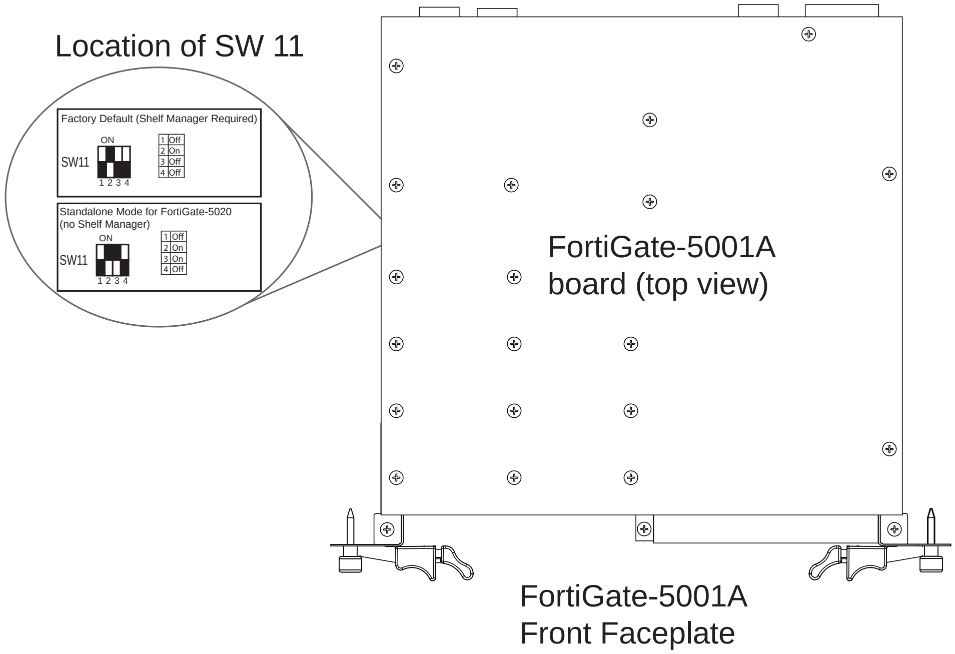
2 If you have installed the FortiGate-5001A board in a chassis, remove it.

For removal instructions, see “Removing a FortiGate-5001A board” on page 18.

3 Use Figure 8 to locate SW11 on the FortiGate-5001A board.

The top of the FortiGate-5001A board is covered with a copper heat sink. The printed circuit board is under the copper heat sink. SW11 is located on the printed circuit board and is accessible from the left side of the FortiGate-5001A board under the copper heat sink (see Figure 8).

Figure 8: Location of SW11 on the FortiGate-5001A board



4 If required, change SW11 to the correct setting.

5 Insert the FortiGate-5001A board into a chassis and verify that the board starts up and operates correctly.

For inserting instructions, see “Inserting a FortiGate-5001A board” on page 15.

Note: Figure 8 shows a FortiGate-5001A-DW board. The location of SW-11 is the same on a FortiGate-5001A-SW board.

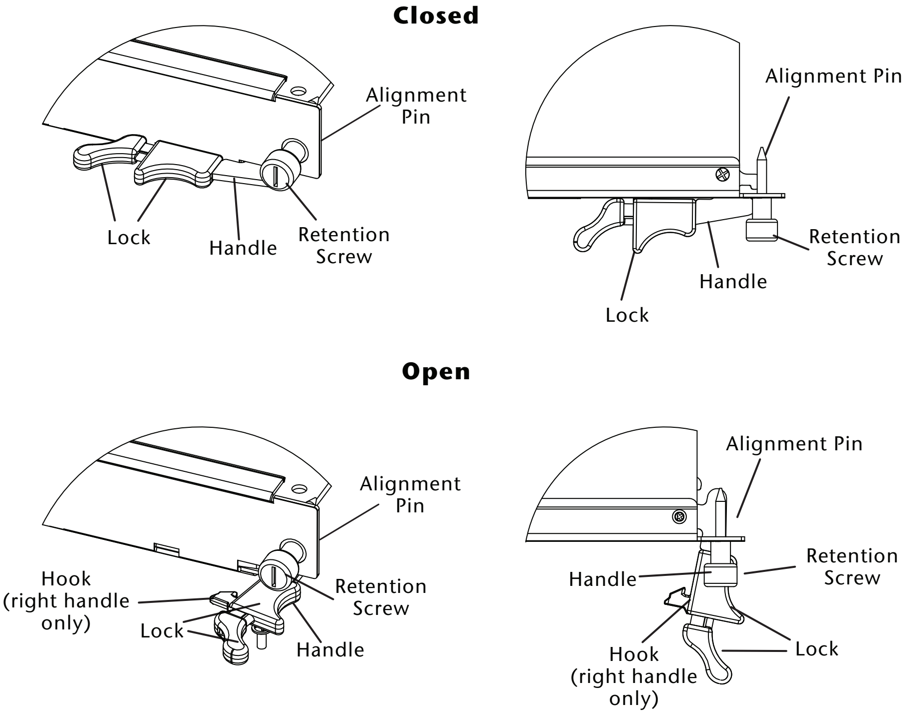
FortiGate-5001A mounting components

To install a FortiGate-5001A board you slide the board into an open slot in the front of an ATCA chassis and then use the mounting components to lock the board into place in the slot. When locked into place and positioned correctly the board front panel is flush with the chassis front panel. The board is also connected to the chassis backplane.

Note: FortiGate-5001A boards are horizontal when inserted into a FortiGate-5050 chassis and vertical when inserted into a FortiGate-5140 chassis. The inserting and removing procedures are the same in either case. For clarity the descriptions in this document refer to the left (top) and right (bottom) mounting components.

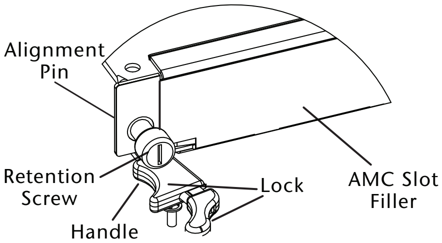
To position the board correctly you must use the mounting components shown in Figure 9 for the right (bottom) side of the front panel. The mounting components on the left (top) side of the FortiGate-5001A-SW front panel are the same but reversed. The mounting components on the left (top) side of the FortiGate-5001A-DW are slightly different as shown in Figure 10. The FortiGate-5001A mounting components align the board in the chassis slot and are used to insert and eject the board from the slot.

Figure 9: FortiGate-5001A right (bottom) mounting components



Note: The FortiGate-5001A-DW right (bottom) handle includes a hook that secures the handle into place when the board is mounted in the chassis (Figure 9). The hook is not included on the FortiGate-5001A-DW left (top) handle (Figure 10). Otherwise the left (top) and right (bottom) mounting components are the same. Operating the left (top) and right (bottom) handles is also basically the same except that without the hook you do not have to squeeze the FortiGate-5001A-DW left (top) handle lock. Also the FortiGate-5001A-DW left (top) handle does not lock into place in the same way as the right (bottom) handle. Both FortiGate-5001A-SW handles include the hook. The hook was removed from the FortiGate-5001A-DW left (top) handle because of the double-width AMC opening.

Figure 10: FortiGate-5001A-DW left (top) mounting components



Inserting a FortiGate-5001A board

The FortiGate-5001A board must be fully installed in a chassis slot, with the handles closed and locked and retention screws fully tightened for the FortiGate-5001A board to receive power and operate normally. If the FortiGate-5001A board is not receiving power, the IPM LED glows solid blue and all other LEDs remain off. See “Front panel LEDs and connectors” on page 6.

It is important to carefully seat the FortiGate-5001A board all the way into the chassis, to not use too much force on the handles, and to make sure that the handles are properly locked. Only then will the FortiGate-5001A board power-on and start up correctly.

FortiGate-5001A boards are hot swappable. The procedure for inserting a FortiGate-5001A board into a chassis slot is the same whether or not the chassis is powered on.

To insert a FortiGate-5001A board into a chassis slot

⚠ **Caution:** Do not carry the FortiGate-5001A board by holding the handles or retention screws. When inserting or removing the FortiGate-5001A board from a chassis slot, handle the board by the front panel. The handles are not designed for carrying the board. If the handles become bent or damaged the FortiGate-5001A board may not align correctly in the chassis slot.

⚠ **Caution:** If you are installing a FortiGate-RTM-XB2 module you must install the FortiGate-RTM-XB2 module first, before you install the FortiGate-5001A board to avoid possible damage. Follow the instructions in the *FortiGate-RTM-XB2 System Guide* to install the FortiGate-RTM-XB2 module.

To complete this procedure, you need:

- A FortiGate-5001A board with either the correct AMC slot filler panel or a FortiGate AMC module installed in the front panel AMC opening
- An ATCA chassis with an empty slot
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

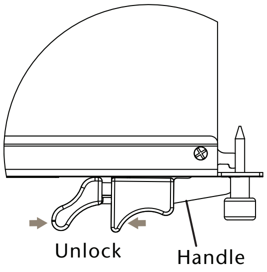
⚠ **Caution:** FortiGate-5001A boards must be protected from static discharge and physical shock. Only handle or work with FortiGate-5001A boards at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate-5001A boards.

1 Attach the ESD wrist strap to your wrist and to an available ESD socket or wrist strap terminal.

2 If required, remove the protective metal frame that the FortiGate-5001A board has been shipped in.

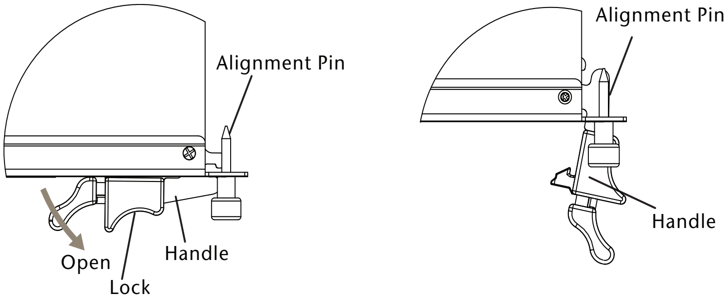
3 Insert the FortiGate-5001A board into the empty slot in the chassis.

4 Unlock the handles by squeezing the handle locks.



5 Open the handles to their fully open positions.

Caution: To avoid damaging the lock, make sure you squeeze the handles fully to unlock them before opening. The handles should pop easily out of the board front panel.



6 Insert the FortiGate-5001A board into the empty slot in the chassis.

7 Carefully guide the board into the chassis using the rails in the slot.

Insert the board by applying moderate force to the front faceplate (not the handles) to slide the board into the slot. The board should glide smoothly into the chassis slot. If you encounter any resistance while sliding the board in, the board could be aligned incorrectly. Pull the board back out and try inserting it again.

8 Slide the board in until the alignment pins are inserted half way into their sockets in the chassis.

9 Turn both handles to their fully-closed positions.

The handles should hook into the sides of the chassis slot. Closing the handles draws the FortiGate-5001A board into place in the chassis slot and into full contact with the chassis backplane. The FortiGate-5001A front panel should be in contact with the chassis front panel. For the FortiGate-5001A-DW, the right (bottom) handle locks into place. For the FortiGate-5001A-SW, both handles lock into place.

As the handles closed power is supplied to the board. If the chassis is powered on the IPM LED starts flashing blue. If the board is aligned correctly, inserted all the way into the slot, and the handles are properly closed the IPM LED flashes blue for a few seconds. At the same time the STATUS LED flashes green, the interface LEDs flash amber, and the ACC LED starts flashing green. After a few seconds the IPM LED goes out and the FortiGate-5001A firmware starts up. During start up the STATUS LED may continue to flash green. Once the board has started up and is operating correctly, the front panel LEDs are lit as described in Table 4.

Table 4: FortiGate-5001A normal operating LEDs

LED	State
ACC	Off (Or flashing green when the system accesses the FortiGate-5001A flash disk.)
OOS (Out of Service)	Off
Power	Green
Status	Off
IPM	Off

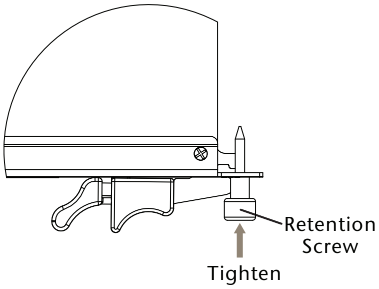
If you have installed an AMC module in the FortiGate-5001A board, the AMC LEDs are lit as described in Table 5.

Table 5: FortiGate AMC module normal operating LEDs

LED	State
HS	Off
OOS	Off
PWR	Amber
OT	Off

If the board has not been inserted properly the IPM LED changes to solid blue and all other LEDS turn off. If this occurs, open the handles, slide the board part way out, and repeat the insertion process.

10 Once the board is inserted correctly, fully tighten the retention screws to lock the FortiGate-5001A board into position in the chassis slot.



Removing a FortiGate-5001A board

The following procedure describes how to correctly use the FortiGate-5001A mounting components described in "FortiGate-5001A mounting components" on page 14 to remove a FortiGate-5001A board from an ATCA chassis slot.

FortiGate-5001A boards are hot swappable. The procedure for removing a FortiGate-5001A board from a chassis slot is the same whether or not the chassis is powered on.

To remove a FortiGate-5001A board from a chassis slot

⚠ **Caution:** Do not carry the FortiGate-5001A board by holding the handles or retention screws. When inserting or removing the FortiGate-5001A board from a chassis slot, handle the board by the front panel. The handles are not designed for carrying the board. If the handles become bent or damaged the FortiGate-5001A board may not align correctly in the chassis slot.

To complete this procedure, you need:

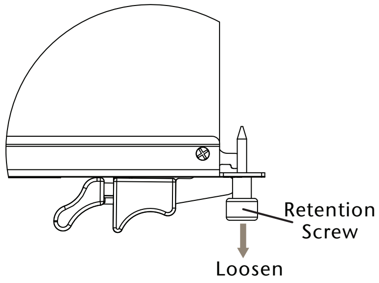
- An ATCA chassis with a FortiGate-5001A board installed
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

⚠ **Caution:** FortiGate-5001A boards must be protected from static discharge and physical shock. Only handle or work with FortiGate-5001A boards at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate-5001A boards.

1 Attach the ESD wrist strap to your wrist and to an available ESD socket or wrist strap terminal.

2 Disconnect all cables from the FortiGate-5001A board, including all network cables, the console cable, and any USB cables or keys.

3 Fully loosen the retention screws on the FortiGate-5001A front panel.

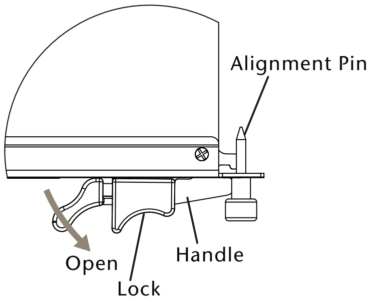


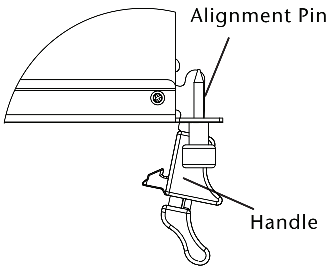
4 Unlock the handles by squeezing the handle locks.

5 Open the handles to their fully open positions.

Caution: To avoid damaging the lock, make sure you squeeze the handles fully to unlock them before opening. The handles should pop easily out of the board front panel.

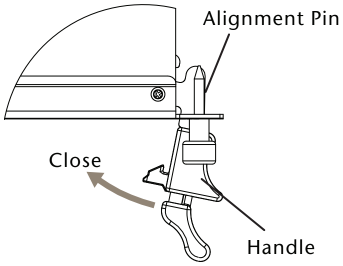
You need to open the handles with moderate pressure to eject the board from the chassis. Pivoting the handles turns off the microswitch, turns off all LEDs, and ejects the board from the chassis slot.

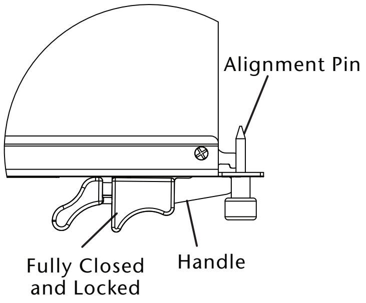




6 Pull the board about half way out.

7 Turn both handles to their fully-closed positions.





8 Carefully slide the board completely out of the slot.

9 Re-attach the protective metal frame before shipping or storing the FortiGate-5001A board.

Resetting a FortiGate-5001A board

You must eject the FortiGate-5001A board from the chassis slot to cycle the power and reset the board. See “Removing a FortiGate-5001A board” on page 18 for information about how to eject a FortiGate-5001A board from a chassis.

Installing and removing AMC modules

This section describes installing a FortiGate AMC Double width Module (ADM) in the FortiGate-5001A-DW front panel AMC double-width opening or a FortiGate AMC Single width Module (ASM) in the FortiGate-5001A-SW front panel AMC single-width opening.

⚠ **Caution:** Do not operate the FortiGate-5001A board with an open AMC opening. For optimum cooling performance and safety, the AMC opening must contain a slot filler panel or a FortiGate AMC module.

⚠ **Caution:** Because the FortiGate-5001A board does not support hot swapping AMC modules, you must eject the FortiGate-5001A board from its chassis slot and completely open the handles before inserting or removing AMC modules or slot filler panels.

Table 6: FortiGate AMC module LEDs

LED	State	Description
HS	Off	Normal operation.
	Blue	Ejection latch open.
	Flashing	The module is starting up or shutting down.
OOS	Off	LED currently not in use.
PWR	Amber	The module is properly inserted in the FortiGate unit.
	Off	The module is not receiving power from the FortiGate unit.
OT	Off	LED currently not in use.
LINK	Green	The correct cable is in use and the connected equipment has power.
	Off	No link established.
ACT	Flashing Green or Amber	Network activity at this interface.
	Off	No network activity at this interface.
ACT/RDY	Amber	The module is properly inserted in the FortiGate unit.
	Off	The module is not receiving power from the FortiGate unit.
PORT	Off	LED currently not in use.

This section describes:

- Inserting AMC slot filler panels
- Inserting AMC modules
- Removing AMC modules

Inserting AMC slot filler panels

The following procedure describes how to install a slot filler panel in the FortiGate-5001A front panel AMC opening. The FortiGate-5001A-DW board includes one AMC double-width slot filler panel and the FortiGate-5001A-SW board includes one AMC single-width slot filler panel.

⚠ **Caution:** Do not operate the FortiGate-5001A board with an open AMC opening. For optimum cooling performance and safety, the AMC opening must contain a slot filler panel or a FortiGate AMC module.

⚠ **Caution:** Because the FortiGate-5001A board does not support hot swapping AMC modules, you must eject the FortiGate-5001A board from its chassis slot and completely open the handles before inserting or removing AMC modules or slot filler panels.

To install an AMC slot filler panel

To complete this procedure, you need:

- FortiGate-5001A board with an empty AMC slot
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

⚠ **Caution:** FortiGate-5001A boards must be protected from static discharge and physical shock. Only handle or work with FortiGate-5001A boards at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate-5001A boards.

1. Attach the ESD wrist strap to your wrist and to an available ESD socket or wrist strap terminal.
2. Eject the FortiGate-5001A board from the chassis slot.
3. With the FortiGate-5001A left (top) handle fully open, pull the latch on the slot filler front panel to the extended position.
4. Insert the slot filler panel by applying moderate force to the front faceplate to slide the slot filler panel into the opening.

   The slot filler panel should glide smoothly into the opening. If you encounter any resistance while sliding the slot filler panel in, the slot filler panel could be aligned incorrectly. Pull the slot filler panel back out and try inserting it again.
5. Press the latch in the slot filler front panel to lock in the slot filler panel.

Inserting AMC modules

The following procedure describes how to install an AMC module into your FortiGate-5001A front panel AMC opening. Insert the fiber transceivers into the module before inserting the module into the FortiGate unit. For details on installing the transceivers, see the *QuickStart Guide* for the AMC module.

To insert an AMC module into a FortiGate-5001A board

⚠ **Caution:** Do not operate the FortiGate-5001A board with an open AMC opening. For optimum cooling performance and safety, the AMC opening must contain a slot filler panel or a FortiGate AMC module.

⚠ **Caution:** Because the FortiGate-5001A board does not support hot swapping AMC modules, you must eject the FortiGate-5001A board from its chassis slot and completely open the handles before inserting or removing AMC modules or slot filler panels.

To complete this procedure, you need:

- A FortiGate-5001A board with an open slot
- FortiGate AMC module to install
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

Caution: FortiGate-5001A boards and FortiGate AMC modules must be protected from static discharge and physical shock. Only handle or work with these components at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling these components.

1. Attach the ESD wrist strap to your wrist and to an available ESD socket or wrist strap terminal.
2. Eject the FortiGate-5001A board from the chassis slot.
3. With the FortiGate-5001A left (top) handle fully open remove the AMC slot filler panel from the FortiGate-5001A front panel by pulling open the latch on the AMC slot filler front panel and then pulling the slot filler panel out using the latch.
4. Pull the latch on the FortiGate AMC module front panel to the extended position.
5. With the FortiGate-5001A left (top) handle fully open, insert the FortiGate AMC module into the empty slot in the FortiGate-5001A front panel. Make sure the Fortinet logo on the module front panel is right-side up. The Fortinet logo appears on the upper-right corner of the module front panel.
6. Carefully guide the module into the FortiGate-5001A board.
7. Insert the module by applying moderate force to the front faceplate near the upper edge to slide the module into the opening.

   The module should glide smoothly into the opening. If you encounter any resistance while sliding the module in, the module could be aligned incorrectly. Pull the module back out and try inserting it again.
8. Press the latch on the module front panel to lock in the module.
9. Insert the FortiGate-5001A board into a chassis slot.

Removing AMC modules

Before removing an AMC module you need to shut down the FortiGate-5001A board using proper shut down procedures.

To remove an AMC module from a FortiGate-5001A board

Caution: Do not operate the FortiGate-5001A board with an open AMC opening. For optimum cooling performance and safety, the AMC opening must contain a slot filler panel or a FortiGate AMC module.

Caution: Because the FortiGate-5001A board does not support hot swapping AMC modules, you must eject the FortiGate-5001A board from its chassis slot and completely open the handles before inserting or removing AMC modules or slot filler panels.

To complete this procedure, you need:

- A FortiGate-5001A board containing a FortiGate AMC module
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

⚠ **Caution:** FortiGate-5001A boards and FortiGate AMC modules must be protected from static discharge and physical shock. Only handle or work with these components at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling these components.

1. Attach the ESD wrist strap to your wrist and to an available ESD socket or wrist strap terminal.
2. Eject the FortiGate-5001A board from the chassis slot.
3. With the FortiGate-5001A left (top) handle fully open, pull the latch on the AMC module front panel to the extended position to unlock the module from the FortiGate-5001A board.
4. Gently pull the latch to remove the module.
5. With the FortiGate-5001A left (top) handle fully open, install a replacement AMC module or an AMC slot filler panel into the opening in the FortiGate-5001A front panel.

Troubleshooting

This section describes the following troubleshooting topics:

- FortiGate-5001A does not start up
- FortiGate-5001A status LED is flashing during system operation
- FortiGate AMC modules not detected by FortiGate-5001A board

FortiGate-5001A does not start up

Shelf manager or firmware problems may prevent a FortiGate-5001A board from starting up correctly.

Chassis with a shelf manager: no communication with shelf manager

If the FortiGate-5001A board is receiving power and the handles are fully closed and the FortiGate-5001A still does not start up, the problem could be that the FortiGate-5001A cannot communicate with the chassis shelf manager. This problem can only occur in an ATCA chassis that contains a shelf manager (such as the FortiGate-5140 and FortiGate-5050).

To correct this problem power down and then restart the chassis. If you are operating a FortiGate-5000 series chassis you can power down and then restart the chassis without removing FortiGate-5000 series components.

All chassis: Firmware problem

If the FortiGate-5001A board is receiving power and the handles are fully closed, and you have restarted the chassis and the FortiGate-5001A still does not start up, the problem could be with FortiOS. Connect to the FortiGate-5001A console and try cycling the power to the board. If the BIOS starts up, interrupt the BIOS startup and install a new firmware image. For details about installing a new firmware image in this way, see the *FortiGate-5000 Series Firmware and FortiUSB Guide*.

If this does not solve the problem, contact Fortinet Technical Support.

FortiGate-5001A status LED is flashing during system operation

Normally, the FortiGate-5001A Status LED ◉ is off when the FortiGate-5001A board is operating normally. If this LED starts flashing while the board is operating, a fault condition may exist. At the same time the FortiGate-5001A may stop processing traffic.

To resolve the problem you can try removing and reinserting the FortiGate-5001A board in the chassis slot. Reloading the firmware may also help.

If this does not solve the problem there may have been a hardware failure or other problem. Contact Fortinet Technical Support for assistance.

FortiGate AMC modules not detected by FortiGate-5001A board

If the FortiGate-5001A board cannot detect the FortiGate AMC module installed in the FortiGate-5001A front panel AMC opening, the AMC module interfaces will not be visible from the FortiGate-5001A web-based manager or CLI. Also, the AMC module HS LED could be solid blue.

To correct this problem you should remove and re-insert the AMC module. Because AMC modules are not hot swappable, you must first remove the FortiGate-5001A board.

⚠ **Caution:** Do not operate the FortiGate-5001A board with an open AMC opening. For optimum cooling performance and safety, the AMC opening must contain a slot filler panel or a FortiGate AMC module.

⚠ **Caution:** Because the FortiGate-5001A board does not support hot swapping AMC modules, you must eject the FortiGate-5001A board from its chassis slot and completely open the handles before inserting or removing AMC modules or slot filler panels.

To remove and reset an AMC module

1. Attach an ESD wrist strap to your wrist and to an ESD socket or to a bare metal surface on the chassis or frame.
2. Remove the FortiGate-5001A board from the chassis slot.

   See “Removing a FortiGate-5001A board” on page 18. You do not have to completely remove the FortiGate-5001A board from the slot; however the board should be disconnected from power.
3. With the FortiGate-5001A left (top) handle fully open, pull the latch on the AMC module front panel to open the latch and pull the AMC module out of the FortiGate-5001A front panel AMC opening.
4. With the FortiGate-5001A left (top) handle fully open, re-insert the AMC module into the FortiGate-5001A front panel AMC opening.

   Make sure the AMC module is inserted correctly into the opening.
5. Close the latch on the AMC front panel.
6. Insert the FortiGate-5001A board into the chassis slot.

   Both the AMC module and the FortiGate-5001A board should start up. If both the FortiGate-5001A board and the AMC module are functioning normally, the front panel LEDs will appear as described in Table 4 on page 17 and Table 5 on page 17.
7. If this does not solve the problem, contact Fortinet Technical Support.

Quick Configuration Guide

This section is a quick start guide to connecting and configuring a FortiGate-5001A security system for your network.

Before using this chapter, your FortiGate-5000 series or compatible ATCA chassis should be mounted and connected to your power system. In addition, your FortiGate-5001A boards should be inserted into the chassis and additional hardware components (such as AMC cards and SFP transceivers) should be installed. The FortiGate-5001A boards should also be powered up and the front panel LEDs should indicate that the boards are functioning normally.

This chapter includes the following topics:

Registering your Fortinet product

Register your Fortinet product to receive Fortinet customer services such as product updates and technical support. You must also register your product for FortiGuard services such as FortiGuard Antivirus and Intrusion Prevention updates and for FortiGuard Web Filtering and AntiSpam.

Register your product by visiting http://support.fortinet.com and selecting Product Registration.

To register, enter your contact information and the serial numbers of the Fortinet products that you or your organization have purchased. You can register multiple Fortinet products in a single session without re-entering your contact information.

Planning the configuration

Before beginning to configure your FortiGate-5001A security system, you need to plan how to integrate the system into your network. Your configuration plan depends on the operating mode that you select: NAT/Route mode (the default) or Transparent mode.

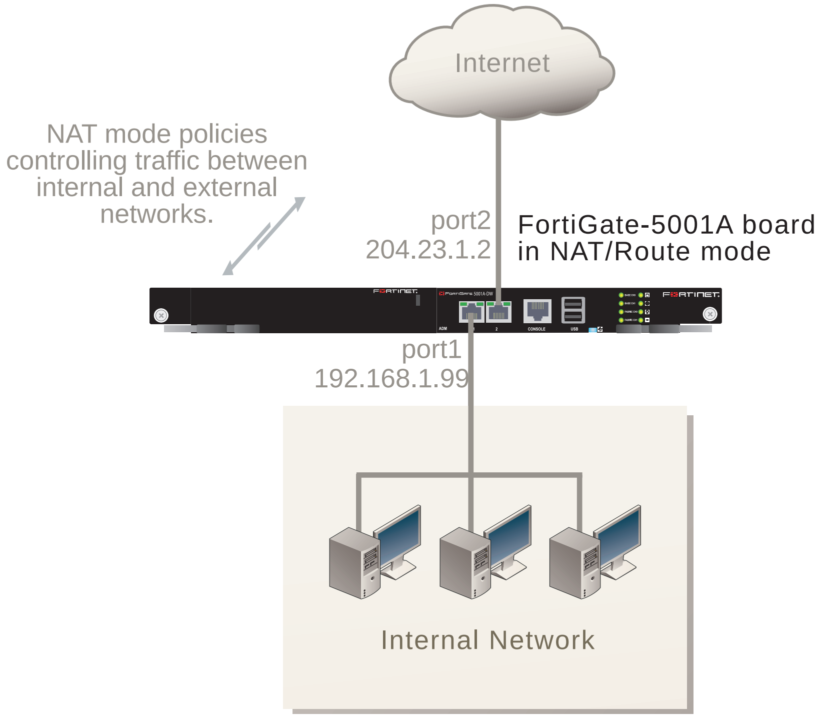
NAT/Route mode

In NAT/Route mode, the FortiGate-5001A security system is visible to the networks that it is connected to. Each interface connected to a network must be configured with an IP address that is valid for that network. In many configurations, in NAT/Route mode all of the FortiGate interfaces are on different networks, and each network is on a separate subnet.

You would typically use NAT/Route mode when the FortiGate-5001A security system is deployed as a gateway between private and public networks. In the default NAT/Route mode configuration, the FortiGate-5001A security system functions as a firewall. Firewall policies control communications through the FortiGate-5001A security system. No traffic can pass through the FortiGate-5001A security system until you add firewall policies.

In NAT/Route mode, firewall policies can operate in NAT mode or in Route mode. In NAT mode, the FortiGate firewall performs network address translation before IP packets are sent to the destination network. In Route mode, no translation takes place.

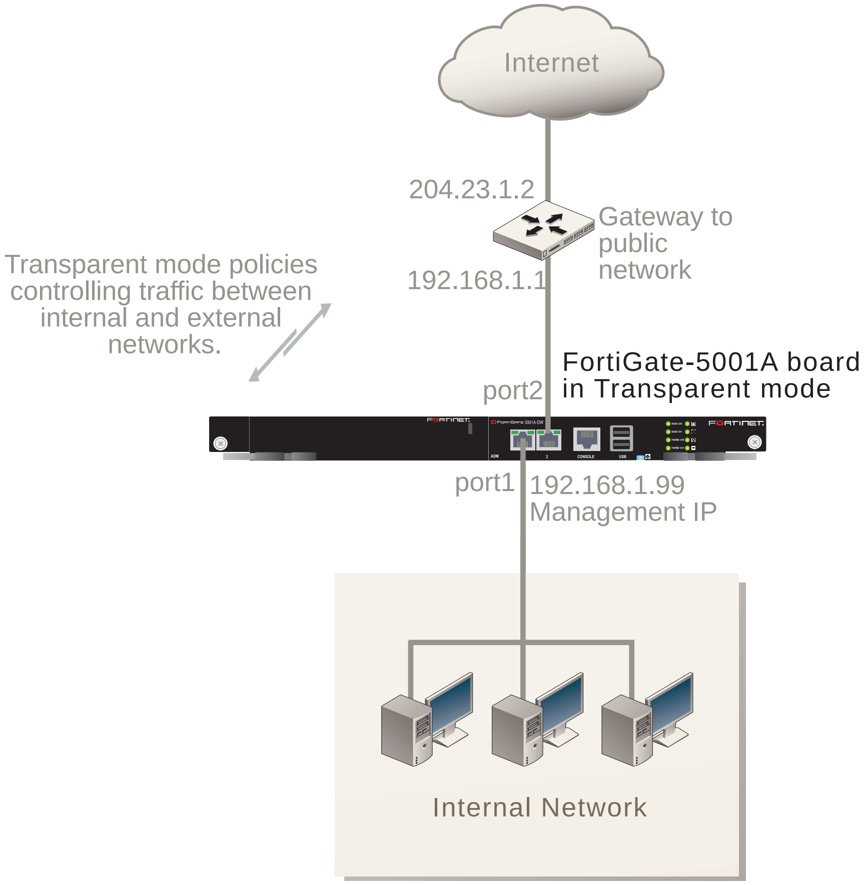
Figure 11: Example FortiGate-5001A board operating in NAT/Route mode


Internet
NAT mode policies controlling traffic between internal and external networks.
port2
204.23.1.2
FortiGate-5001A board in NAT/Route mode
port1
192.168.1.99
Internal Network

Transparent mode

In Transparent mode, the FortiGate-5001A security system is invisible to the network. All of the FortiGate-5001A interfaces are connected to different segments of the same network. In Transparent mode you only have to configure a management IP address so that you can connect to the FortiGate-5001A security system to make configuration changes and so the FortiGate-5001A security system can connect to external services such as the FortiGuard Distribution Network (FDN).

Figure 12: Example FortiGate-5001A board operating in Transparent mode


Internet
204.23.1.2
Gateway to public network
192.168.1.1
Transparent mode policies controlling traffic between internal and external networks.
FortiGate-5001A board in Transparent mode
port2
port1
192.168.1.99
Management IP
Internal Network

You would typically deploy a FortiGate-5001A security system in Transparent mode on a private network behind an existing firewall or behind a router. In the default Transparent mode configuration, the FortiGate-5001A security system functions as a firewall. No traffic can pass through the FortiGate-5001A security system until you add firewall policies.

Choosing the configuration tool

You can use either the web-based manager or the Command Line Interface (CLI) to configure the FortiGate board.

Web-based manager

The FortiGate-5001A web-based manager is an easy to use management tool. Use the web-based manager to configure the FortiGate-5001A administrator password, the interface addresses, the default gateway, and the DNS server addresses.

Requirements:

- An Ethernet connection between the FortiGate-5001A board and management computer.
- Internet Explorer 6.0 or higher on the management computer.

Command Line Interface (CLI)

The CLI is a full-featured management tool. Use it to configure the administrator password, the interface addresses, the default gateway, and the DNS server addresses.

Requirements:

- The serial connector that came packaged with your FortiGate-5001A board.
- Terminal emulation application (for example, HyperTerminal for Windows) on the management computer.

Factory default settings

The FortiGate-5001A unit ships with a factory default configuration. The default configuration allows you to connect to and use the FortiGate-5001A web-based manager to configure the FortiGate-5001A board onto the network. To configure the FortiGate-5001A board onto the network you add an administrator password, change the network interface IP addresses, add DNS server IP addresses, and, if required, configure basic routing.

Table 7: FortiGate-5001A factory default settings

Operation Mode	NAT/Route
Administrator Account	User Name: admin Password: (none)
port1 IP/Netmask	192.168.1.99/24
port2 IP/Netmask	192.168.100.99/24
Default route	Gateway: 192.168.100.1 Device: port2
Primary DNS Server:	65.39.139.53
Secondary DNS Server:	65.39.139.53

Note: At any time during the configuration process, if you run into problems, you can reset the FortiGate-5001A board to the factory defaults and start over. From the web-based manager go to **System > Status** find System Operation at the bottom of the page and select Reset to Factory Default. From the CLI enter `execute factory reset`.

Configuring NAT/Route mode

Use Table 8 to gather the information you need to customize NAT/Route mode settings for the FortiGate-5001A security system. You can use one table for each board to configure.

Table 8: FortiGate-5001A board NAT/Route mode settings

Admin Administrator Password:		
port1	IP:	______.______.______.______
	Netmask:	______.______.______.______
port2	IP:	______.______.______.______
	Netmask:	______.______.______.______
Default Route	Device (Name of the Interface connected to the external network):	
	Default Gateway IP address:	______.______.______.______
	The default route consists of the name of the interface connected to an external network (usually the Internet) and the default gateway IP address. The default route directs all non-local traffic to this interface and to the external network.	
DNS Servers	Primary DNS Server:	______.______.______.______
	Secondary DNS Server:	______.______.______.______

Using the web-based manager to configure NAT/Route mode

1. Connect port1 of the FortiGate-5001A board to the same hub or switch as the computer you will use to configure the FortiGate board.

Note: If you cannot connect to port1, see “Using the CLI to configure NAT/Route mode” on page 30.

2. Configure the management computer to be on the same subnet as the port1 interface of the FortiGate-5001A board. To do this, change the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.
3. To access the FortiGate web-based manager, start Internet Explorer and browse to https://192.168.1.99 (remember to include the “s” in https://).
4. Type admin in the Name field and select Login.

To change the admin administrator password

1. Go to **System > Admin > Administrators**.
2. Select Change Password for the admin administrator and enter a new password.

Note: See the Fortinet Knowledge Center article Recovering lost administrator account passwords if you forget or lose an administrator account password and cannot log into your FortiGate unit.

To configure interfaces

1. Go to **System > Network > Interface**.
2. Select the edit icon for each interface to configure.

3 Set the addressing mode for the interface. (See the online help for information.)

- For manual addressing, enter the IP address and netmask for the interface that you added to Table 8 on page 29.
- For DHCP addressing, select DHCP and any required settings.
- For PPPoE addressing, select PPPoE and enter the username and password and any other required settings.

To configure the Primary and Secondary DNS server IP addresses

1 Go to **System > Network > Options**.

2 Enter the Primary and Secondary DNS IP addresses that you added to Table 8 on page 29 as required and select Apply.

To configure the Default Gateway

1 Go to **Router > Static** and select Edit icon for the static route.

2 Select the Device that you recorded above.

3 Set Gateway to the Default Gateway IP address that you added to Table 8 on page 29.

4 Select OK.

Using the CLI to configure NAT/Route mode

1 Use the serial cable supplied with your FortiGate-5001A board to connect the FortiGate Console port to the management computer serial port.

2 Start a terminal emulation program (HyperTerminal) on the management computer. Use these settings:

Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.

3 At the Login: prompt, type admin and press Enter twice (no password required).

4 Change the administrator password.

```
config system admin
  edit admin
      set password <password>
  end
```

Note: See the Fortinet Knowledge Center article Recovering lost administrator account passwords if you forget or lose an administrator account password and cannot log into your FortiGate unit.

5 Configure the port1 internal interface to the setting that you added to Table 8 on page 29.

```
config system interface
  edit port1
      set ip <intf_ip>/<netmask_ip>
  end
```

6 Repeat to configure each interface as required, for example, to configure the port2 interface to the setting that you added to Table 8 on page 29.

```
config system interface
   edit port2
   ...
```

7 Configure the primary and secondary DNS server IP addresses to the settings that you added to Table 8 on page 29.

```
config system dns
   set primary <dns-server_ip>
   set secondary <dns-server_ip>
   end
```

8 Configure the default gateway to the setting that you added to Table 8 on page 29.

```
config router static
   edit 1
        set device <interface_name>
        set gateway <gateway_ip>
   end
```

Configuring Transparent mode

Use Table 9 to gather the information you need to customize Transparent mode settings.

Table 9: Transparent mode settings

Admin Administrator Password:		
Management IP	IP:	_____._____._____._____
	Netmask:	_____._____._____._____
	The management IP address and netmask must be valid for the network where you will manage the FortiGate-5001A unit.	
Default Route	Default Gateway IP address:	_____._____._____._____
	In Transparent mode the default route requires the default gateway IP address. The default route directs all non-local traffic to the external network.	
DNS Servers	Primary DNS Server:	_____._____._____._____
	Secondary DNS Server:	_____._____._____._____

Using the web-based manager to configure Transparent mode

1 Connect port1 of the FortiGate-5001A board to the same hub or switch as the computer you will use to configure the FortiGate board.

Note: If you cannot connect to port1, see "Using the CLI to configure Transparent mode" on page 32.

2 Configure the management computer to be on the same subnet as the port1 interface of the FortiGate-5001A board. To do this, change the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.

3 To access the FortiGate web-based manager, start Internet Explorer and browse to https://192.168.1.99 (remember to include the "s" in https://).

4 Type admin in the Name field and select Login.

To switch from NAT/Route mode to transparent mode

1 Go to **System > Status** and select the Change link beside Operation Mode: NAT.

2 Set Operation Mode to Transparent.

3 Set the Management IP/Netmask to the settings that you added to Table 9 on page 31.

4 Set the default Gateway to the setting that you added to Table 9 on page 31.

To change the admin administrator password

1 Go to **System > Admin > Administrators**.

2 Select Change Password for the admin administrator and enter the password that you added to Table 9 on page 31.

To change the management interface

1 Go to **System > Config > Operation**.

2 Enter the Management IP address and netmask hat you added to Table 9 on page 31 and select Apply.

To configure the Primary and Secondary DNS server IP addresses

1 Go to **System > Network > Options**.

2 Enter the Primary and Secondary DNS IP addresses that you added to Table 9 on page 31 as required and select Apply.

Using the CLI to configure Transparent mode

1 Use the serial cable supplied with your FortiGate-5001A board to connect the FortiGate Console port to the management computer serial port.

2 Start a terminal emulation program (HyperTerminal) on the management computer. Use these settings:

Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.

3 At the Login: prompt, type admin and press Enter twice (no password required).

4 Change from NAT/Route mode to Transparent mode. Configure the Management IP address and default gateway to the settings that you added to Table 9 on page 31.

```
config system settings
  set opmode transparent
  set manageip <mng_ip>/<netmask>
  set gateway <gateway_ip>
  end
```

5 Configure the primary and secondary DNS server IP addresses to the settings that you added to Table 9 on page 31.

```
config system dns
  set primary <dns-server_ip>
  set secondary <dns-server_ip>
  end
```

Upgrading FortiGate-5001A firmware

Fortinet periodically updates the FortiGate-5001A FortiOS firmware to include enhancements and address issues. After you have registered your FortiGate-5001A security system (see “Registering your Fortinet product” on page 25) you can download FortiGate-5001A firmware from the support web site http://support.fortinet.com.

Only FortiGate-5001A administrators (whose access profiles contain system read and write privileges) and the FortiGate-5001A admin user can change the FortiGate-5001A firmware.

For complete details about upgrading and downgrading FortiGate-5001A firmware using the web-based manager or CLI; and using a USB key, see the *FortiGate-5000 Series Firmware and FortiUSB Guide*.

To upgrade the firmware using the web-based manager

1. Copy the firmware image file to your management computer.
2. Log into the web-based manager as the admin administrator.
3. Go to **System > Status**.
4. Under **System Information > Firmware Version**, select Update.
5. Type the path and filename of the firmware image file, or select Browse and locate the file.
6. Select OK.

   The FortiGate-5001A board uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.
7. Log into the web-based manager.
8. Go to **System > Status** and check the Firmware Version to confirm the firmware upgrade is successfully installed.
9. Update the FortiGate-5001A antivirus and attack definitions. See the FortiGate-5001A online help for details.

To upgrade the firmware using the CLI

To use the following procedure, you must have a TFTP server the FortiGate-5001A board can connect to.

1. Make sure the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log into the CLI.
4. Make sure the FortiGate board can connect to the TFTP server.

   You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```
5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate-5001A board:

   ```
   execute restore image <name_str> <tftp_ipv4>
   ```

Where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image image.out 192.168.1.168
```

The FortiGate-5001A board responds with the message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

6 Type y.

The FortiGate-5001A board uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

7 Reconnect to the CLI.

8 To confirm the firmware image is successfully installed, enter:

```
get system status
```

9 Update antivirus and attack definitions. You can use the command

```
execute update-now
```

FortiGate-5001A base backplane data communication

This section describes how to configure FortiGate-5001A boards for base backplane data communication. Base backplane data communication is supported for FortiGate-5001A boards installed in FortiGate-5140, FortiGate-5050, and FortiGate-5020 chassis.

Note: Different FortiGate-5000 series boards may use different names for the base backplane interfaces. For example, on the FortiGate-5001SX and FortiGate-5001FA2 boards the base backplane interfaces are called port9 and port10. On the FortiGate-5005FA2 and FortiGate-5001A boards, the base backplane interfaces are called base1 and base2.

By default the base backplane interfaces are not enabled for data communication. Once the base backplane interfaces are configured for data communication you can operate and configure them in the same way as any FortiGate-5001A interfaces.

Note: The FortiSwitch-5003 board does not support VLAN-tagged packets.

Note: The FortiSwitch-5003A board and the FortiGate-5020 backplane do support VLAN-tagged packets.

Although not recommended, you can use base backplane interfaces for data communication and HA heartbeat communication at the same time.

In a FortiGate-5140 or FortiGate-5050 chassis, FortiGate-5001A base backplane communication requires one or two FortiSwitch-5003A or FortiSwitch-5003 boards. A FortiSwitch board installed in chassis base slot 1 provides communication on the base1 interface. A FortiSwitch-5003 board installed in chassis base slot 2 provides communication on the base2 interface. The FortiGate-5020 chassis supports base backplane data communication for both interfaces with no additions or changes to the chassis.

Note: Installing a FortiSwitch-5003A board and a FortiSwitch-5003 board in the same chassis is not supported.

For details and configuration examples of FortiGate-5001A base backplane communication using the FortiSwitch-5003 board, see the *FortiGate-5000 Backplane Communications Guide*.

To enable base backplane data communication from the FortiGate-5001A web-based manager

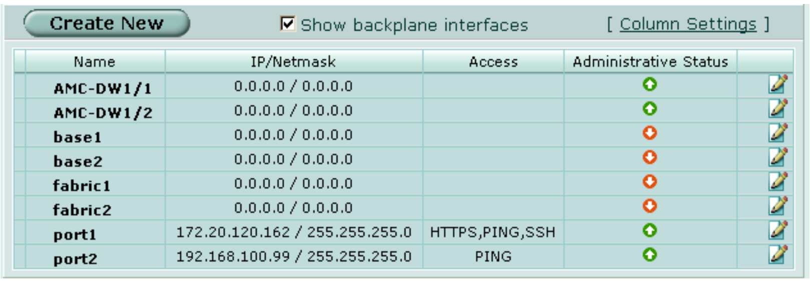
From the FortiGate-5001A web-based manager use the following steps to enable base backplane data communication.

1 Go to **System > Network > Interface**.

2 Select Show backplane interfaces.

The base1 and base2 backplane interfaces now appear in all Interface lists. You can now configure the base backplane interfaces and add routes, firewall policies and other configuration settings using these interfaces.

Figure 13: FortiGate-5001A interface list with backplane interfaces enabled (FortiGate-ADM-XB2 also installed)



Name	IP/Netmask	Access	Administrative Status	
AMC-DW1/1	0.0.0.0 / 0.0.0.0		▲	✎
AMC-DW1/2	0.0.0.0 / 0.0.0.0		▲	✎
base1	0.0.0.0 / 0.0.0.0		▼	✎
base2	0.0.0.0 / 0.0.0.0		▼	✎
fabric1	0.0.0.0 / 0.0.0.0		▼	✎
fabric2	0.0.0.0 / 0.0.0.0		▼	✎
port1	172.20.120.162 / 255.255.255.0	HTTPS,PING,SSH	▲	✎
port2	192.168.100.99 / 255.255.255.0	PING	▲	✎

To enable base backplane data communication from the FortiGate-5001A CLI

From the FortiGate-5001A board CLI you can use the following steps to enable base backplane data communication.

1 Enter the following command to show the backplane interfaces:

```
config system global
   set show-backplane-intf enable
   end
```

The base1 and base2 backplane interfaces now appear in all Interface lists. You can now configure the base backplane interfaces and add routes, firewall policies and other configuration settings using these interfaces.

FortiGate-5001A fabric backplane data communication

This section describes how to configure FortiGate-5001A boards for fabric backplane data communication using the fabric1 and fabric2 interfaces. Fabric backplane data communication is supported for FortiGate-5001A boards installed in FortiGate-5140 and FortiGate-5050 chassis with a FortiSwitch-5003A board installed in chassis fabric slot 1 for the fabric1 interface and a FortiSwitch-5003A board installed in chassis fabric slot 2 for the fabric2 interface.

For the FortiGate-5001A, FortiSwitch-5003A boards support gigabit fabric backplane communication. You can add a FortiGate-RTM-XB2 module to support 10 gigabit fabric backplane communication.

By default the fabric backplane interfaces are not enabled for data communication. Once the fabric backplane interfaces are configured for data communication you can operate and configure them in the same way as any FortiGate-5001A interfaces.

Although not recommended, you can use fabric backplane interfaces for data communication and HA heartbeat communication at the same time.

For more details and configuration examples of FortiGate-5001A fabric backplane communication using the FortiSwitch-5003A board, see the *FortiSwitch-5003A System Guide*.

To enable fabric backplane data communication from the FortiGate-5001A web-based manager

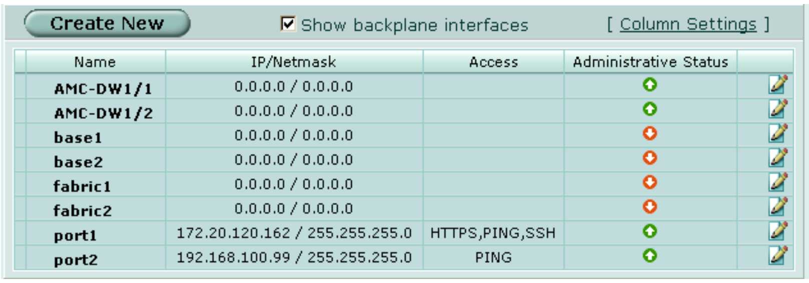
From the FortiGate-5001A web-based manager use the following steps to enable fabric backplane data communication.

1 Go to **System > Network > Interface**.

2 Select Show backplane interfaces.

The fabric1 and fabric2 backplane interfaces now appear in all Interface lists. You can now configure the fabric backplane interfaces and add routes, firewall policies and other configuration settings using these interfaces.

Figure 14: FortiGate-5001A interface list with backplane interfaces enabled (FortiGate-ADM-XB2 also installed)



☑ Show backplane interfaces

Name	IP/Netmask	Access	Administrative Status	
AMC-DW1/1	0.0.0.0 / 0.0.0.0		⬆	✎
AMC-DW1/2	0.0.0.0 / 0.0.0.0		⬆	✎
base1	0.0.0.0 / 0.0.0.0		⬇	✎
base2	0.0.0.0 / 0.0.0.0		⬇	✎
fabric1	0.0.0.0 / 0.0.0.0		⬇	✎
fabric2	0.0.0.0 / 0.0.0.0		⬇	✎
port1	172.20.120.162 / 255.255.255.0	HTTPS,PING,SSH	⬆	✎
port2	192.168.100.99 / 255.255.255.0	PING	⬆	✎

To enable fabric backplane data communication from the FortiGate-5001A CLI

From the FortiGate-5001A board CLI you can use the following steps to enable fabric backplane data communication.

1 Enter the following command to show the backplane interfaces:

```
config system global
  set show-backplane-intf enable
  end
```

The fabric1 and fabric2 backplane interfaces now appear in all Interface lists. You can now configure the fabric backplane interfaces and add routes, firewall policies and other configuration settings using these interfaces.

To enable sending heartbeat packets to the FortiSwitch-5003A

Use the following command to enable sending heartbeat packets from the FortiGate-5001A fabric interfaces. A FortiSwitch-5003A board receives the heartbeat packets to verify that the FortiGate-5001A board is still active.

The FortiGate-5001A board sends 10 packets per second from each fabric interface. The packets are type 255 bridge protocol data unit (BPDU) packets.

1 Enter the following command to enable sending heartbeat packets:

```
config system global
  set fortiswitch-heartbeat enable
  end
```

Powering off the FortiGate-5001A board

To avoid potential hardware problems, always shut down the FortiGate-5001A operating system properly before removing the FortiGate-5001A board from a chassis slot or before powering down the chassis.

To power off a FortiGate-5001A board

1 Shut down the FortiGate-5001A operating system:

- From the web-based manager, go to **System > Status** and from the **Unit Operation** widget, select Shutdown and then select OK.
- From the CLI enter `execute shutdown`

2 Remove the FortiGate-5001A board from the chassis slot.

Note: Once a shutdown operation is completed, the only way to restart the FortiGate-5001A board is to remove and reinsert it.

For more information

Support for your Fortinet product is available as online help from within the web-based manager, from the Tools and Documentation CD included with the product, on the Fortinet Technical Documentation web site, from the Fortinet Knowledge Center web site, as well as from Fortinet Technical Support.

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at http://docs.forticare.com. FortiGate-5000 series documentation is located in its own section of the site at http://docs.forticare.com/fgt5k.html.

Fortinet Tools and Documentation CD

Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current for your product at shipping time. For the latest versions of all Fortinet documentation see the Fortinet Technical Documentation web site at http://docs.forticare.com.

Fortinet Knowledge Center

Additional information about Fortinet products is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at http://kc.forticare.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

Register your Fortinet product

Register your Fortinet product to receive Fortinet customer services such as product updates and technical support. You must also register your product for FortiGuard services such as FortiGuard Antivirus and Intrusion Prevention updates and for FortiGuard Web Filtering and AntiSpam.

Register your product by visiting http://support.fortinet.com and selecting Product Registration.

To register, enter your contact information and the serial numbers of the Fortinet products that you or your organization have purchased. You can register multiple Fortinet products in a single session without re-entering your contact information.

Trademarks

Regulatory compliance

FCC Class A, Part 15
CE mark
VCCI
C-Tick
UL/CUL

FORTINET®

www.fortinet.com